UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,303	11/17/2003	Dominic Hugo Symes	550-483	1092

23117 7590 07/18/2007

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
07/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,303	SYMES, DOMINIC HUGO	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 29.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As per claim 1, 15 and 29, Applicant asserts a "mode" is different from a "domain" because "as explained in the specification, the secure and non-secure domains provide a mechanism for handling security at the hardware level. They effectively establish separate worlds: the non-secure world groups all hardware and software accessible to non-secure applications that do not require security, and the secure world groups all hardware and software that is only accessible when executing secure code. In contrast, a mode of operation is only available to certain types of devices such as processors. Figures 3 and 4 provide simple illustrations of the difference between modes and domains, and are described at page 18, line 28 to page 19, line 15 repeated here for convenience" (remarks: Page 12, 1st Para). Examiner respectfully notes Applicant's argument has no merit since the alleged limitation has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

4. As per claim 1, Applicant asserts prior-arts does not teach "a storage unit configured to store processor configuration data" (Remarks; Page 14, 2nd Para). Examiner respectfully disagrees because (a) Examiner notes "processor configuration data" is merely interpreted as the configuration data that affects the operation of the processor (such as determining the

access to a particular memory bank with a particular program executed by the processor) and (b) Candelore teaches the MSB-bit of the address register is used as the memory space configuration data to manage the upper / lower memory bank for set of secure or non-secure program domains – e.g. the MSB is set or not determines if the upper memory bank 197 can be used for a set of programs A or the lower memory bank 198 can be used for a set of programs B (Candelore: Page 16 Line 6 – 1, Page 11 Line 16 – 18 and Page 10 Line 21 – 24). Therefore, Candelore does teach "a storage unit configured to store processor configuration data" and as such Applicant's arguments are respectfully traversed.

5. Furthermore, Applicant asserts prior-arts does not teach "monitor mode specific processor configuration data" (Remarks: Page 15, 3rd Para / Last sentence). Examiner notes (a) "processor configuration data" is merely interpreted as the configuration data that affects the operation of the processor (b) Shipman teaches the sleuth mode monitor program works transparently to either a secure or non-secure operating system and is merely directed by the SMI handler – for example, even though the system initially operates in normal mode (i.e. non-secured mode), the SMI handler validates the password (i.e. a secured data) in the monitor mode and determines whether switching to the secured mode or back to the normal mode (Shipman: Column 4 Line 61 – 63, Column 5 Line 52 – 65 and Column 8 Line 64 – 67 & Figure 4). Therefore, the password used by SMI handler in the sleuth monitor mode to determine whether switching to the secured mode or back to the normal mode is considered as the "monitor mode specific processor configuration data", which is also consistent with the disclosure of the specification of the instant application as memory permission data that indicates that the processor is allowed to access said secure data.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 – 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore et al. (WO 01/46800), in view of Shipman et al. (U.S. Patent 5,724,027).

As per claim 1, 15 and 29, Candelore teaches a data processing apparatus, comprising:

a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain (Candelore: Figure 1, Page 5 Line 13 – 19 and Page 8 Line 7 – 24: including a secure system portion and a non-secure system portion), and a monitor mode (Candelore: Page 13 Line 26 – 29: the switching mode between the secure mode and non-secure mode is considered as a monitor mode) , said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode (Candelore: Page 8 Line 7 – 24: not even a single bit of the secure domain is passed / leaked to the non-secure domain);

a storage unit configured to store processor configuration data (Candelore: Page 16 Line 6 – 1, Page 11 Line 16 – 18 and Page 10 Line 21 – 24: for examples – (a) the MSB-bit of the address register is used as the memory space configuration data to manage the upper / lower

memory bank for set of secure or non-secure program domains, or (b) a mode selection signal is used by the mode A / B timer switcher).

Candelore teaches said switching including switching the processor configuration data in the storage unit between secure processor configuration data and non-secure processor configuration data (Candelore: Page 16 Line 6 – 11: for examples – the MSB-bit of the address register is used as the upper / lower memory bank for set of secure or non-secure programs). However, Candelore does not disclose expressly said processor being configured at least partially in said monitor mode to execute a monitor program to manage switching between said secure domain and said non-secure domain.

Shipman teaches said processor being configured at least partially in said monitor mode to execute a monitor program to manage switching between said secure domain and said non-secure domain (Shipman: Figure 4 / Element 106, 104 & 102, Column 2 Line 10 – 28, Column 4 Line 42 – 46: three modes are involved – a secure mode, a normal mode is as non-secure mode and a sleuth mode is qualified as a monitor / tracking mode, where the sleuth mode is directed exclusively by a SMI (System Management Interrupt) to perform the requested switching and mapping accordingly. Therefore, Examiner notes a SMI interrupt handler associated with the sleuth / monitor mode is indeed configured at least partially within the processor to execute a monitor program (i.e. SMI interrupt handler) to manage switching between said secure domain and said non-secure domain).

Accordingly (repeated herein), Candelore in view of Shipman teaches said processor being configured at least partially in said monitor mode to execute a monitor program to manage switching between said secure domain and said non-secure domain, said switching including switching the processor configuration data in the storage unit between secure processor

configuration data and non-secure processor configuration data (repeated herein – See the rationale as set forth above);

when in said monitor mode, said monitor program being configured to use monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data (Shipman: Column 4 Line 61 – 63, Column 5 Line 52 – 65 and Column 8 Line 64 – 67 & Figure 4: the sleuth mode monitor program works transparently to either a secure or non-secure operating system and is merely directed by the SMI handler – for example, even though the system initially operates in normal mode (i.e. non-secured mode), the SMI handler validates the password (i.e. a secured data) in the monitor mode and determines whether switching to the secured mode or back to the normal mode and as such is not controlled (i.e. unaffected) by the switching of the processor configuration data either way. Therefore, Examiner notes a portion of the monitor mode specific processor configuration data is interpreted as memory permission data that indicates that the processor is allowed to access said secure data (e.g. password – secured identity data) in said monitor mode that is also consistent with the disclosure of the specification of the instant application).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shipman within the system of Candelore because (a) Candelore teaches a dual-mode processing allowing a secure and non-secure program domain to be managed within a single processor (Candelore: Page 17 Line 24 – 27 and Column 12 Line 23 – 26) and (b) Shipman teaches providing a more flexible and cost effective mechanism to an enhanced dual-mode processing by using a SMI (System Management Interrupt) directed monitor-mode to make the appropriate security switching so that by virtue of the extendibility of the SMI handler, the system security functions may be easily

extended and allowing minimal functionality to be required of the system and thereby reducing the cost of the system facility (Shipman: Column 2 Line 38 – 45 / 23 – 28).

As per claim 2 and 16, Candelore as modified teaches said processor configuration data is configured to control access to memory by the processor (Candelore: Page 16 Line 6 – 11 and Page 13 Line 26 – Page 14 Line 30: for examples – (a) the MSB-bit of the address register is used as one of the processor configuration data to manage the upper / lower memory bank for set of secure or non-secure programs, or (b) a mode selection signal is used by the mode A / B timer switcher and the options of timing data is used as one of the processor configuration data to manage the switching between the secure and non-secure program domains).

As per claim 3 and 17, Candelore as modified teaches the memory is configured to store data required by the processor and comprises secure memory for storing the secure data and non-secure memory for storing non-secure data (Candelore: Page 8 Line 15 – 24), said processor configuration data comprising memory permission data identifying whether the processor is allowed to access said secure data (Candelore: Page 13 Line 12 – 16 and Page 11 Line 11 – 15: the access control registers are used to allow the access to various memory blocks (either secure or nonsecure)).

As per claim 4 and 18, Candelore as modified teaches said processor configuration data comprises memory space configuration data identifying which areas of memory are accessible by the processor (Candelore: Page 16 Line 6 – 11, Page 11 Line 19 – 22 and Page 10 Line 21 – 24: for examples – the MSB-bit of the address register is used as the memory space

configuration data to manage the upper / lower memory bank for set of secure or non-secure program domains).

As per claim 5 and 19, Candelore as modified teaches said memory includes a tightly coupled memory, and said memory space configuration data includes data for controlling the processor's access to said tightly coupled memory (Candelore: Page 16 Line 1 – 11 and Page 10 Line 21 – 24: cache memory is considered as one type of tightly coupled memories).

As per claim 6 and 20, Candelore as modified teaches said memory includes a cache, and said memory space configuration data includes data for controlling the processor's access to said cache (Candelore: Figure 3 / Element 170 & 190, Page 16 Line 1 – 11 and Page 10 Line 21 – 24: the MSB-bit of the cache address register is used as the memory space configuration data to manage the upper / lower bank A / B of cache memory for set of secure or non-secure program domains).

As per claim 7 and 21, Candelore as modified teaches said storage unit comprises one or more system configuration registers (Candelore: Figure 3 and Page 16 Line 6 – 11).

As per claim 8 and 22, Candelore as modified teaches said monitor mode specific processor configuration data is hard-coded (Candelore: Page 15 Line 13 – 16, Page 11 Line 16 – 18 and Page 14 Line 1 – 12: a mode selection signal is used by the mode A / B timer switcher and the timing requirement (i.e. one of monitor mode specific processor configuration data) can be placed on the CPU – i.e. it is hard coded).

As per claim 9 and 23, Candelore as modified teaches selection logic configured to select between said processor configuration data stored in the storage unit and said monitor mode specific processor configuration data in dependence on a control signal identifying whether the processor is operating in said monitor mode (Candelore: Figure 4 and Page 13 Line 20 – 28: the mode selection signal is qualified as the control signal).

As per claim 10 and 24, Candelore as modified teaches in said at least one non-secure mode the processor is configured under the control of a non-secure operating system and in said at least one secure mode the processor is configured under the control of a secure operating system (Candelore: Page 9 Line 3 – 4 and Page 6 Line 1 – 2 and Figure 1 / Element 10 & 50: two separate O.S.).

As per claim 11 and 25, Candelore as modified teaches said monitor mode specific processor configuration data comprises memory permission data that indicates that the processor is allowed to access said secure data in said monitor mode (Shipman: Column 8 Line 62 – 67 & Candelore: Page 13 Line 12 – 16 and Page 11 Line 11 – 15: in sleuth / monitor mode, the SMI handler is allowed to access the password (i.e. the secure data – user authentication identity data) prior to switching to the non-secured or secure mode based on the result of the authentications. Therefore, Examiner notes a portion of the monitor mode specific processor configuration data is interpreted as memory permission data that indicates that the processor is allowed to access said secure data (e.g. password – secured identity data) in said monitor mode).

As per claim 12 and 26, Candelore as modified teaches a memory management unit configured, upon receipt of a memory access request from the processor, to perform one or more predetermined access control functions to control issuance of the memory access request to the memory (Candelore: Page 11 Line 3 – 15 and Page 13 Line 12 – 16: the secured memory access request is interpreted as the predetermined access control functions to control issuance of the memory access request to meet the claim language); said monitor mode specific processor configuration data indicating that said memory management unit is disabled in said monitor mode (Shipman: Column 8 Line 62 – 67: in sleuth / monitor mode, the SMI handler validates the presented password prior to switching to the secure mode and being allowed to access the primary portion of secured memory according to the result of the authentications and as such Examiner notes the majority portion of secured memories are obviously disabled in said monitor mode and subsequently enabled only after the success of password validation that directs the processor switching to the secured operation mode, as taught by Shipman).

As per claim 13 and 27, Candelore as modified teaches said memory includes a cache (Candelore: Page 11 Line 3 – 15 and Page 13 Line 12 – 16: the secured cache is interpreted as the included cache memory to meet the claim language), and said monitor mode specific processor configuration data indicates that the processor is not allowed to use said cache to access data in said monitor mode (Shipman: Column 8 Line 62 – 67: in sleuth / monitor mode, the SMI handler validates the presented password prior to switching to the secure mode and being allowed to access the primary portion of secured memory according to the result of the authentications and as such Examiner notes the majority portion of secured cache memories are obviously disabled in said monitor mode and subsequently enabled only after the success of

password validation that directs the processor switching to the secured operation mode, as taught by Shipman).

As per claim 14 and 28, Candelore as modified teaches at least a portion of said monitor mode specific processor configuration data is derived from the secure processor configuration data (Shipman: Column 8 Line 62 – 67 & Candelore: Page 13 Line 12 – 16 and Page 11 Line 11 – 15: in sleuth / monitor mode, the SMI handler is allowed to access the password (i.e. the secure data – user authentication identity data) prior to switching to the non-secured or secure mode based on the result of the authentications and as such Examiner notes a portion of the monitor mode specific processor configuration data is interpreted as memory permission data that indicates that the processor is allowed to access said secure data (e.g. password – secured identity data) in said monitor mode, which is also derived from the secure processor configuration data).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100